Setting up the OPAM Audit Module

OPAM logs all security events as auditable data which can be used to get detailed insight of Privileged Account management and thus helps refine and effectively manage their usage.

OPAM can be configured to store audit data in either of the below mentioned repositories.

- File - Audit info are stored in the file system on the OS
- Database - Audit event info is pushed to a Database.

Note:

- None of the audit stores are configured OOTB.
- BI Publisher reporting can be leveraged if the Audit repository is a database

We are going to look at a scenario where a Database can be used to store the audit event information

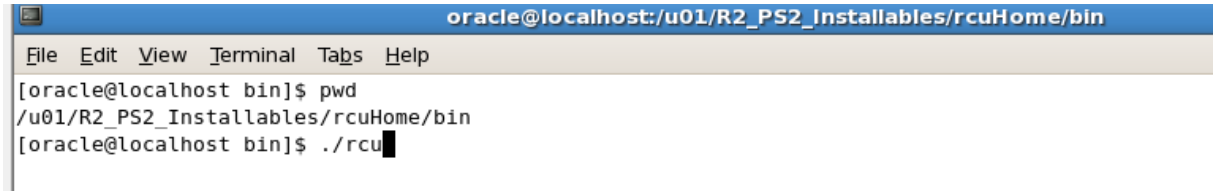
High Level steps

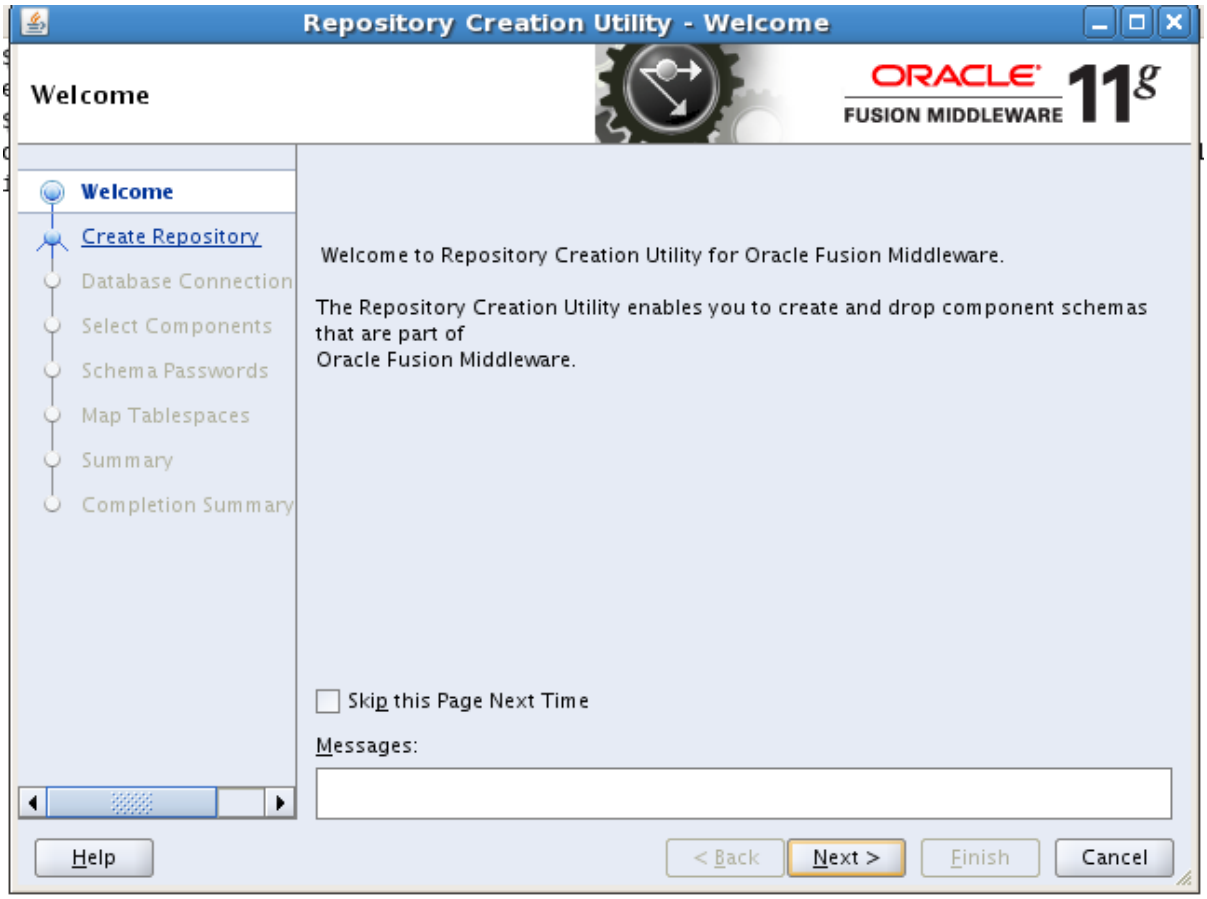
- Create Audit Schema using RCU (http://docs.oracle.com/cd/E29505_01/core.1111/e10043/audpolicy.htm#BABHGBAH)
- Create JDBC Data Source in the OPAM Weblogic Server (providing Audit Schema details)
- Configure OPAM to use Database centric audit logging
- Install BI Publisher
- Configure BI Publisher with Audit Data Store details
- Configure OPAM reports with BI Publisher

1. **Create Audit Schema using RCU**

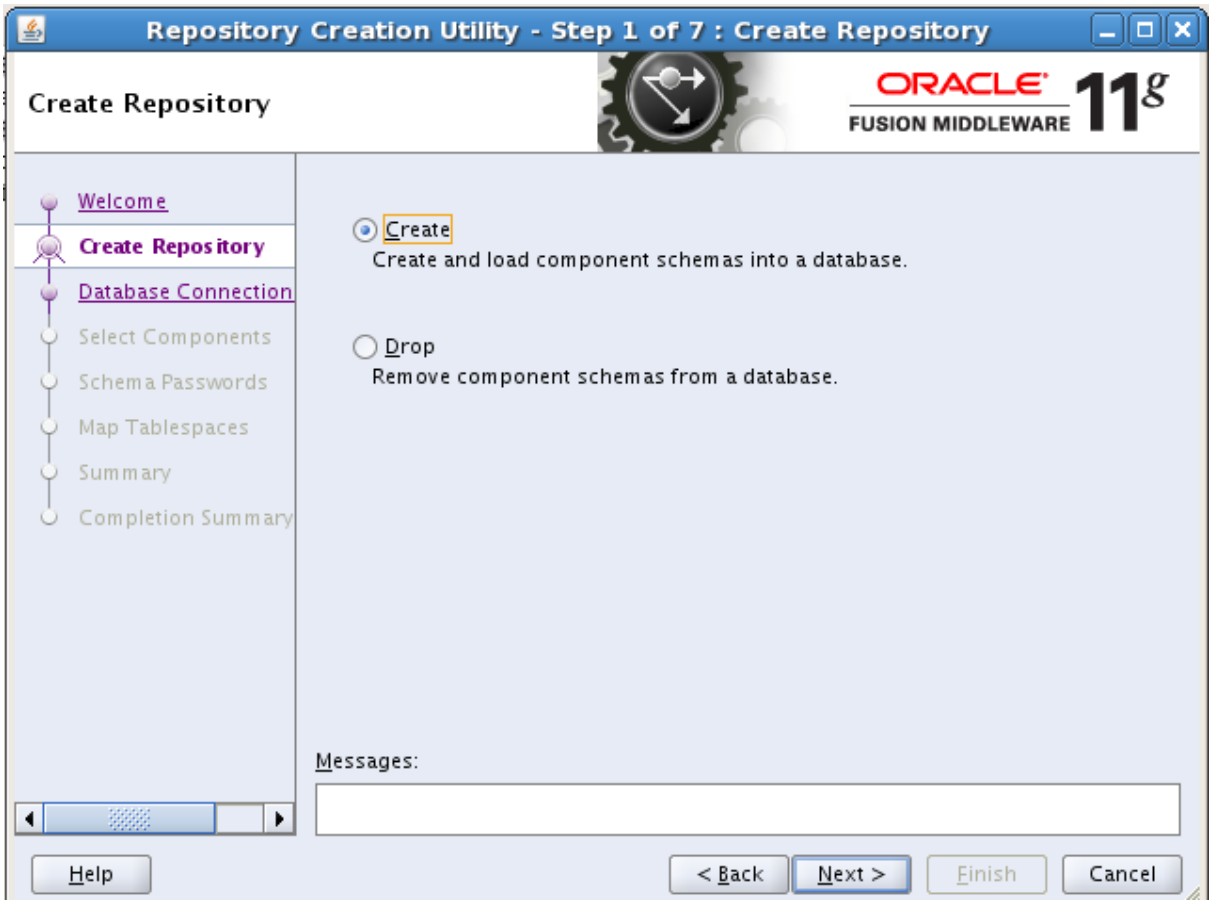
   Execute RCU

   cd /u01/R2_PS2_Installables/rcuHome/bin

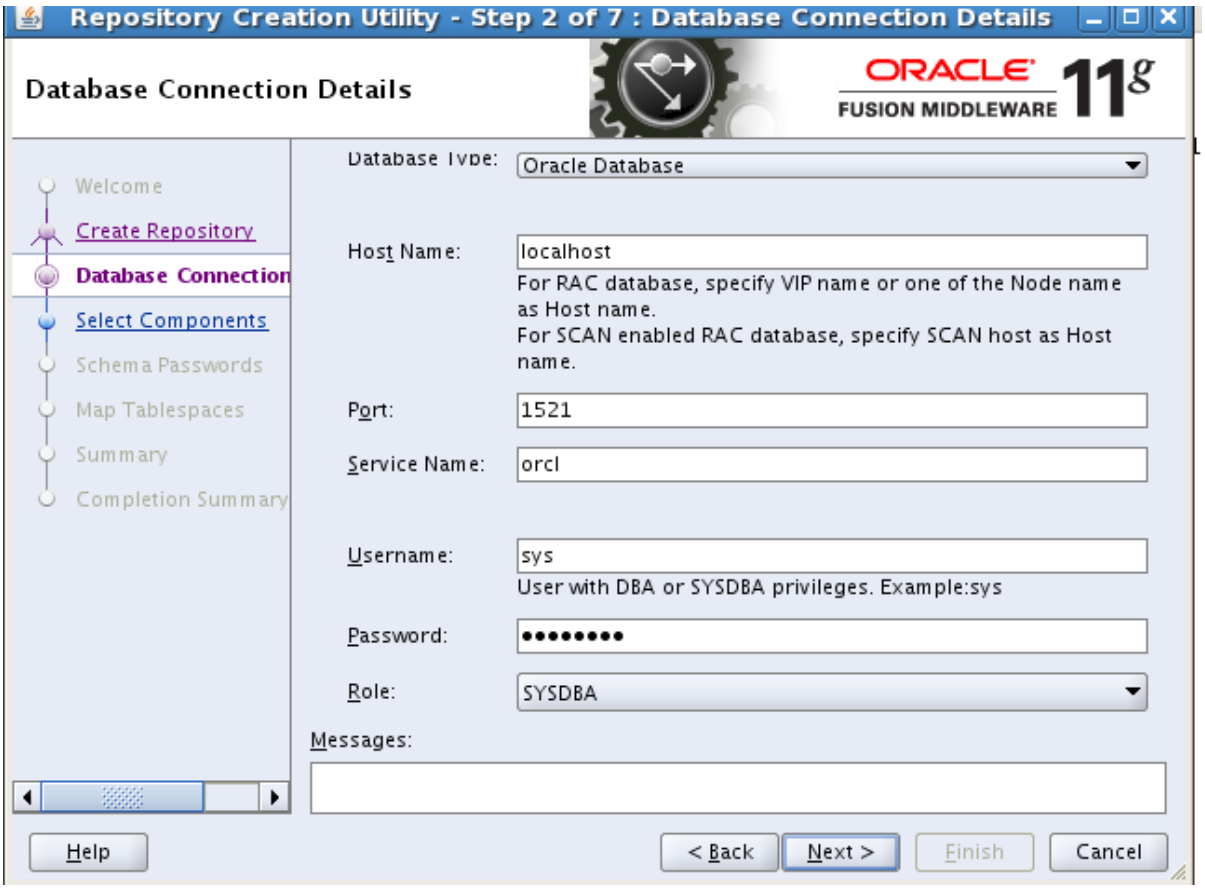




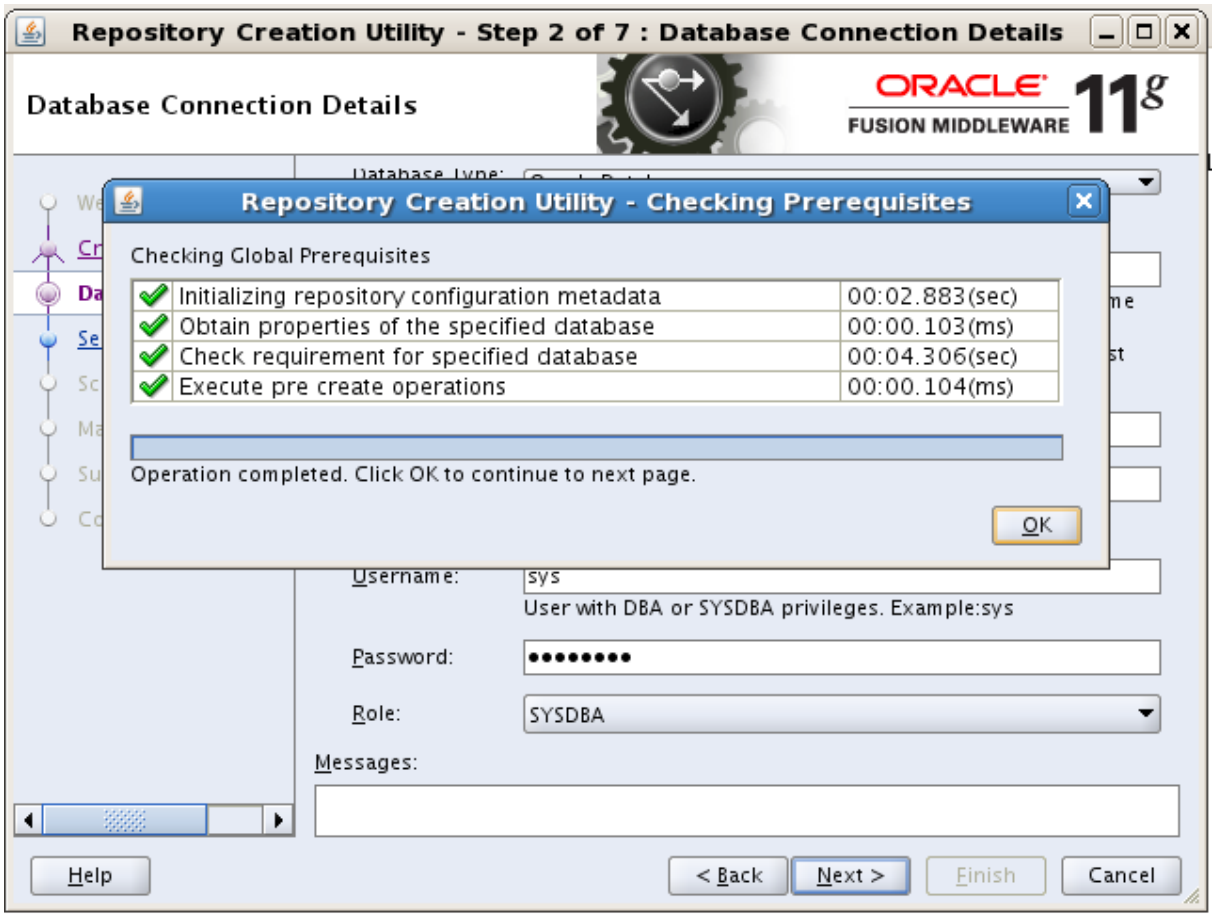
By Abhishek Gupta



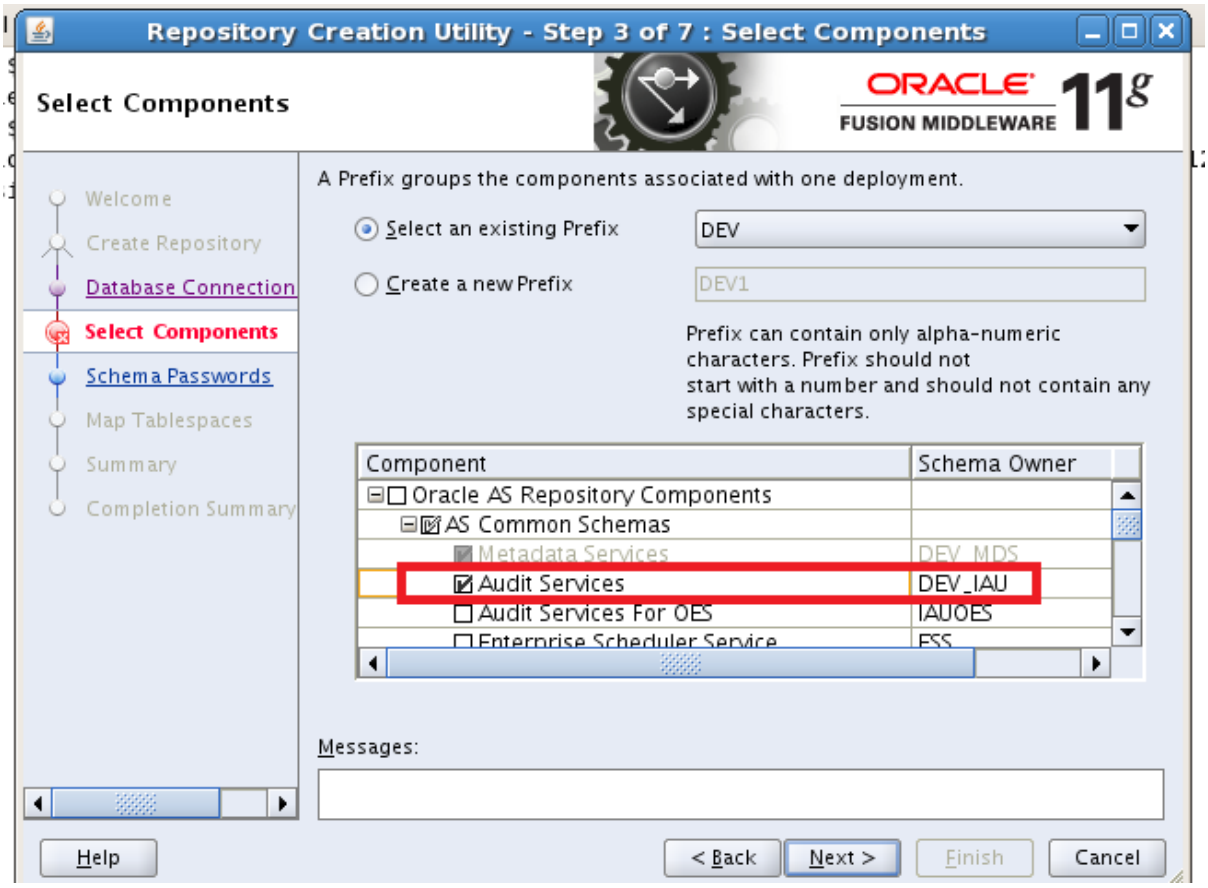
By Abhishek Gupta



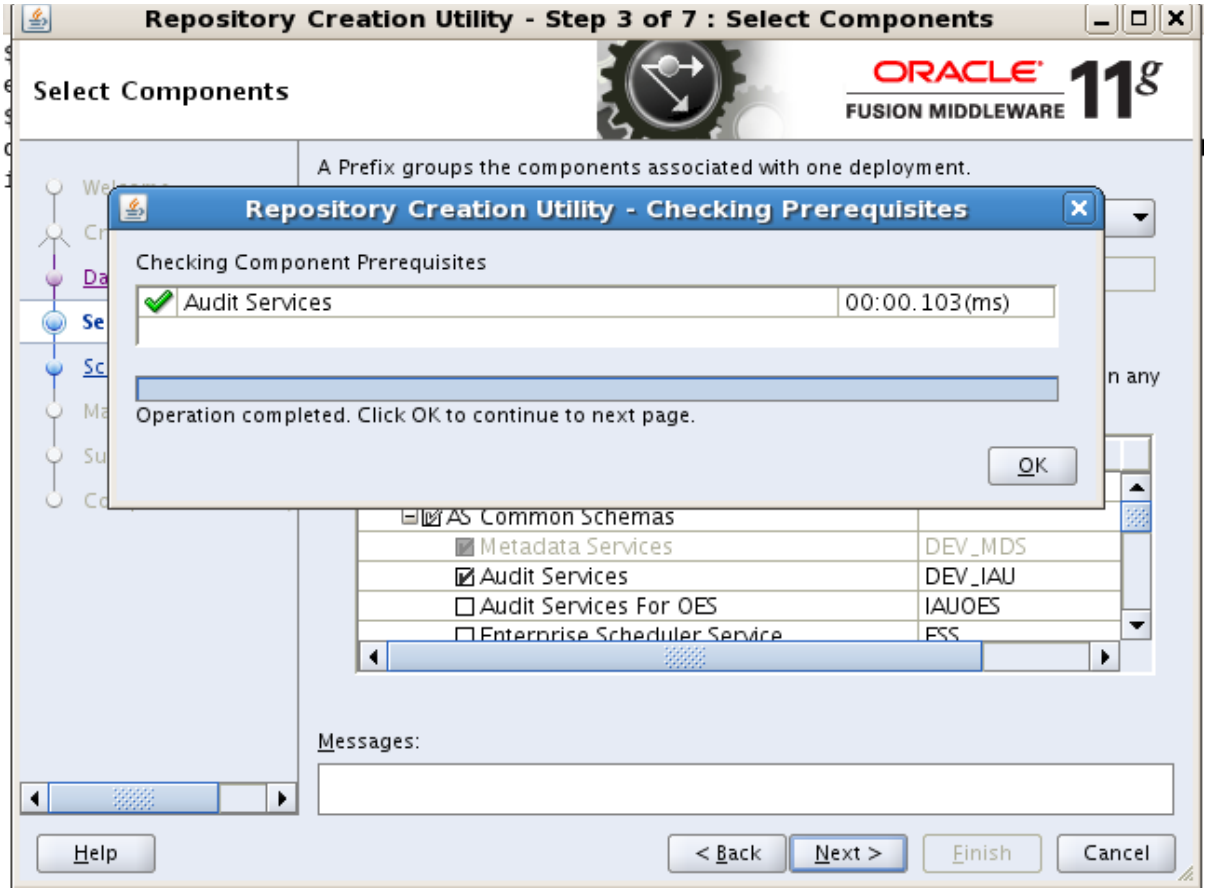
By Abhishek Gupta



Select Audit Services

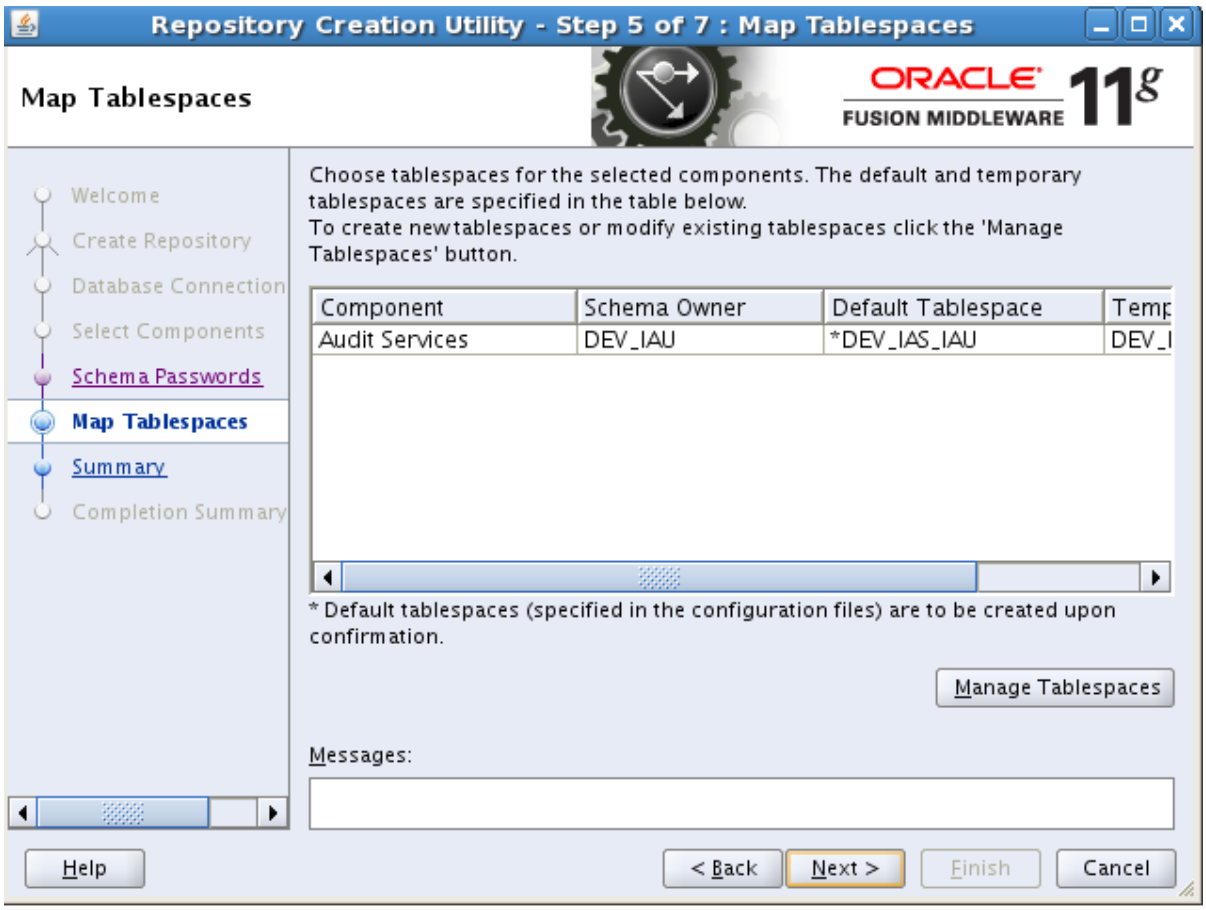


By Abhishek Gupta

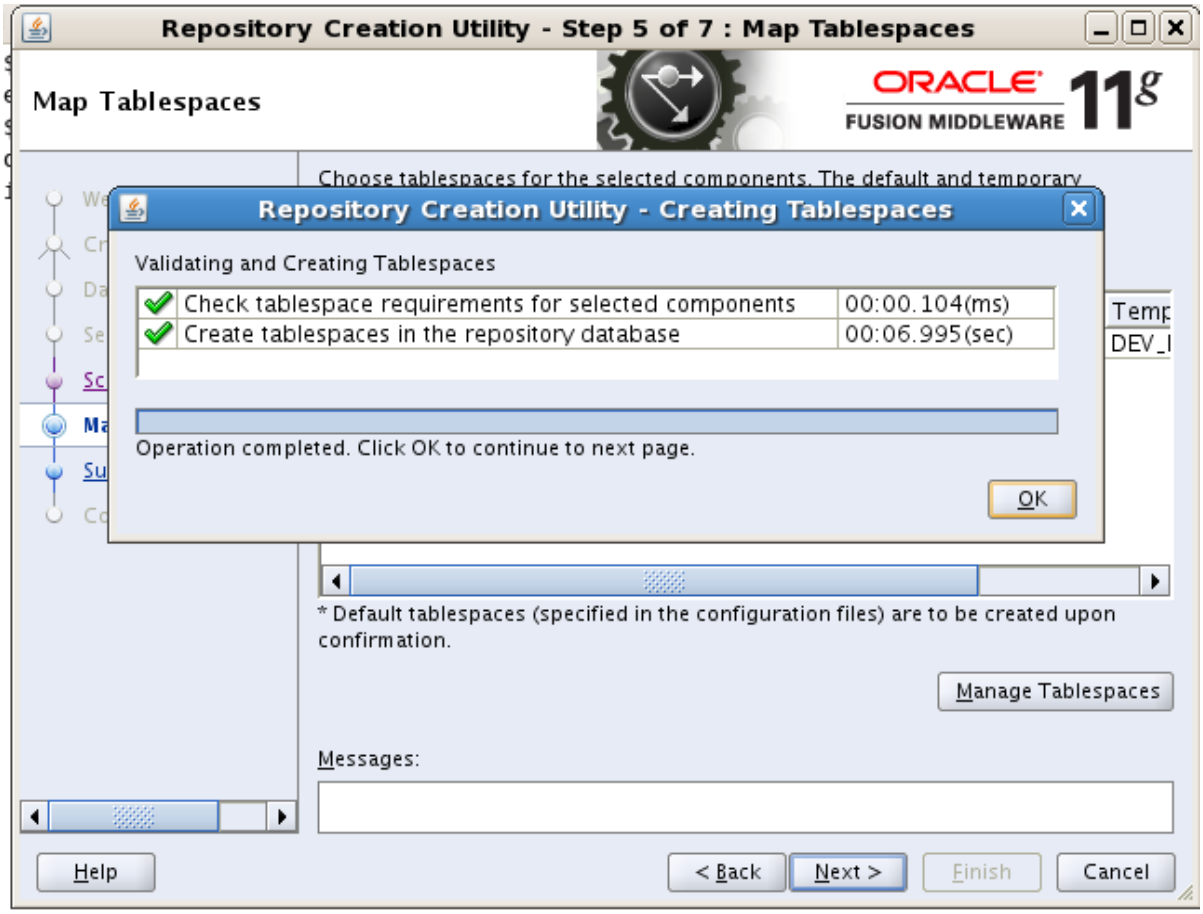


By Abhishek Gupta

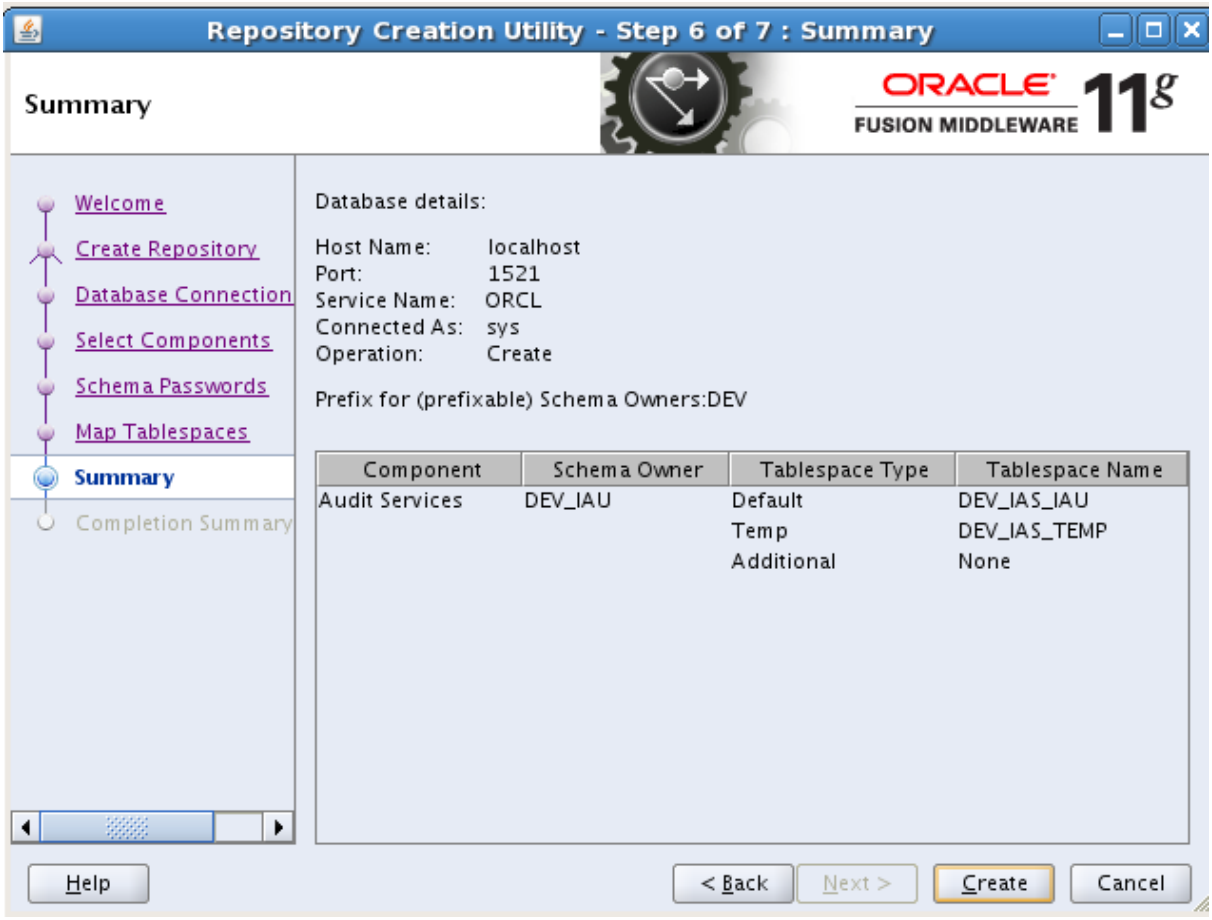
By Abhishek Gupta



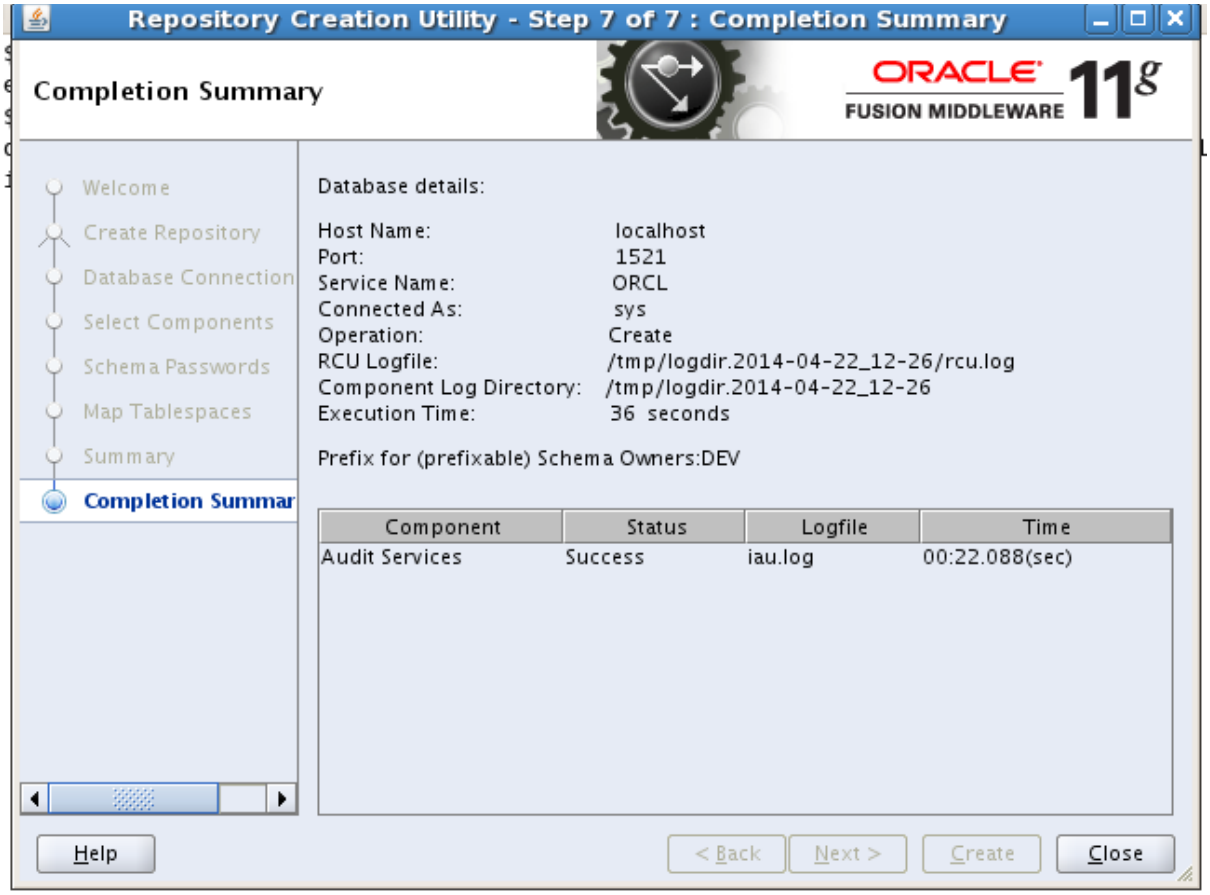
By Abhishek Gupta



By Abhishek Gupta



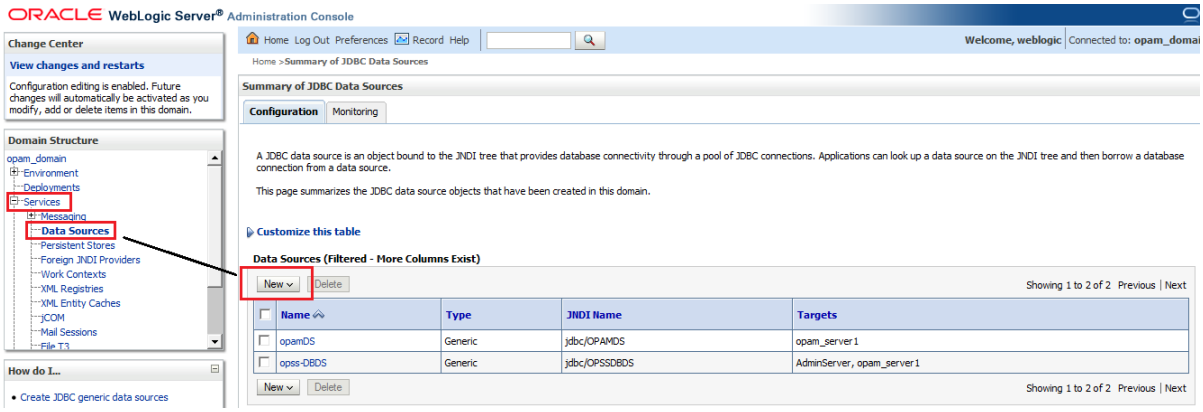
By Abhishek Gupta



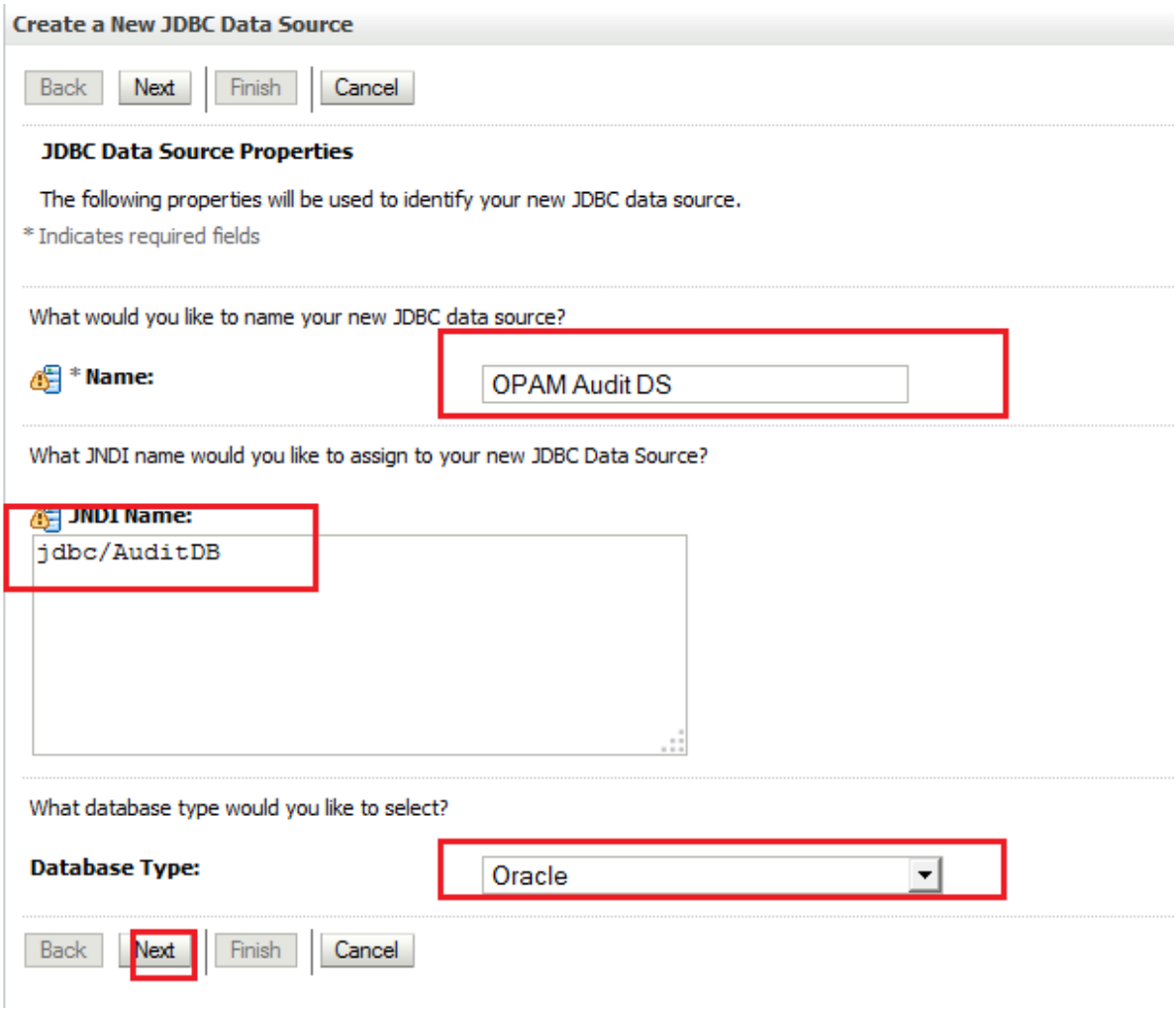
2. **Create JDBC Data Source in the OPAM Weblogic Server**

We will configure and deploy the JDBC data source on both ***OPAM Admin*** and ***managed servers***

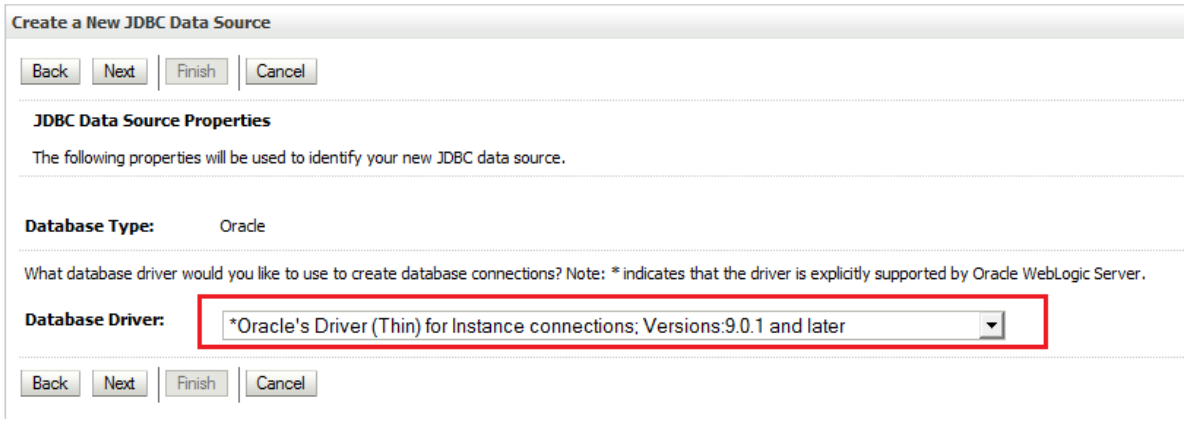
Start OPAM Weblogic Admin and managed servers (if not already running) and then initiate Data Source configuration using steps below



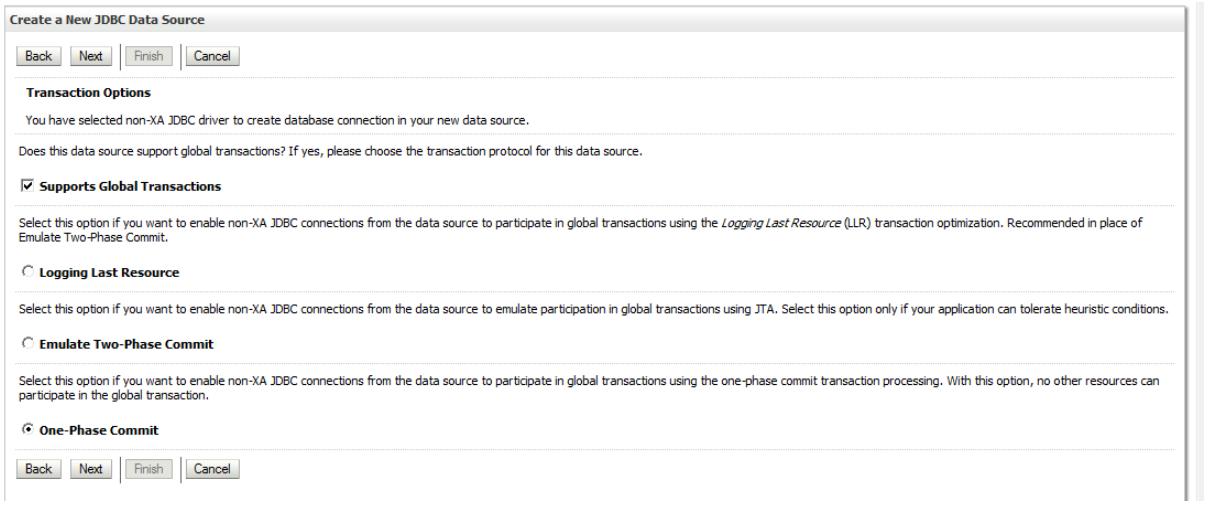
Make sure that the JNDI name for the Data Source is ***jdbc/AuditDB***

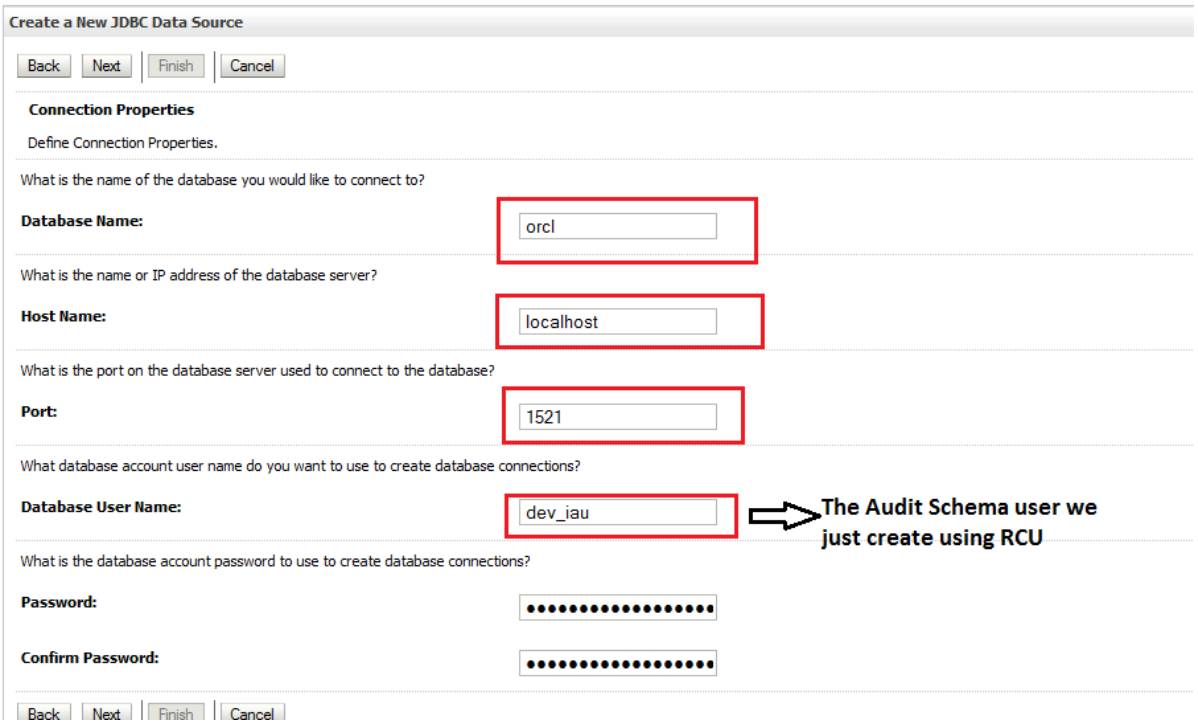

Create a New JDBC Data Source
Back
Next
Finish
Cancel
JDBC Data Source Properties
The following properties will be used to identify your new JDBC data source.
* Indicates required fields
What would you like to name your new JDBC data source?
* Name:
OPAM Audit DS
What JNDI name would you like to assign to your new JDBC Data Source?
JNDI Name:
jdbc/AuditDB
What database type would you like to select?
Database Type:
Oracle
Back
Next
Finish
Cancel

s

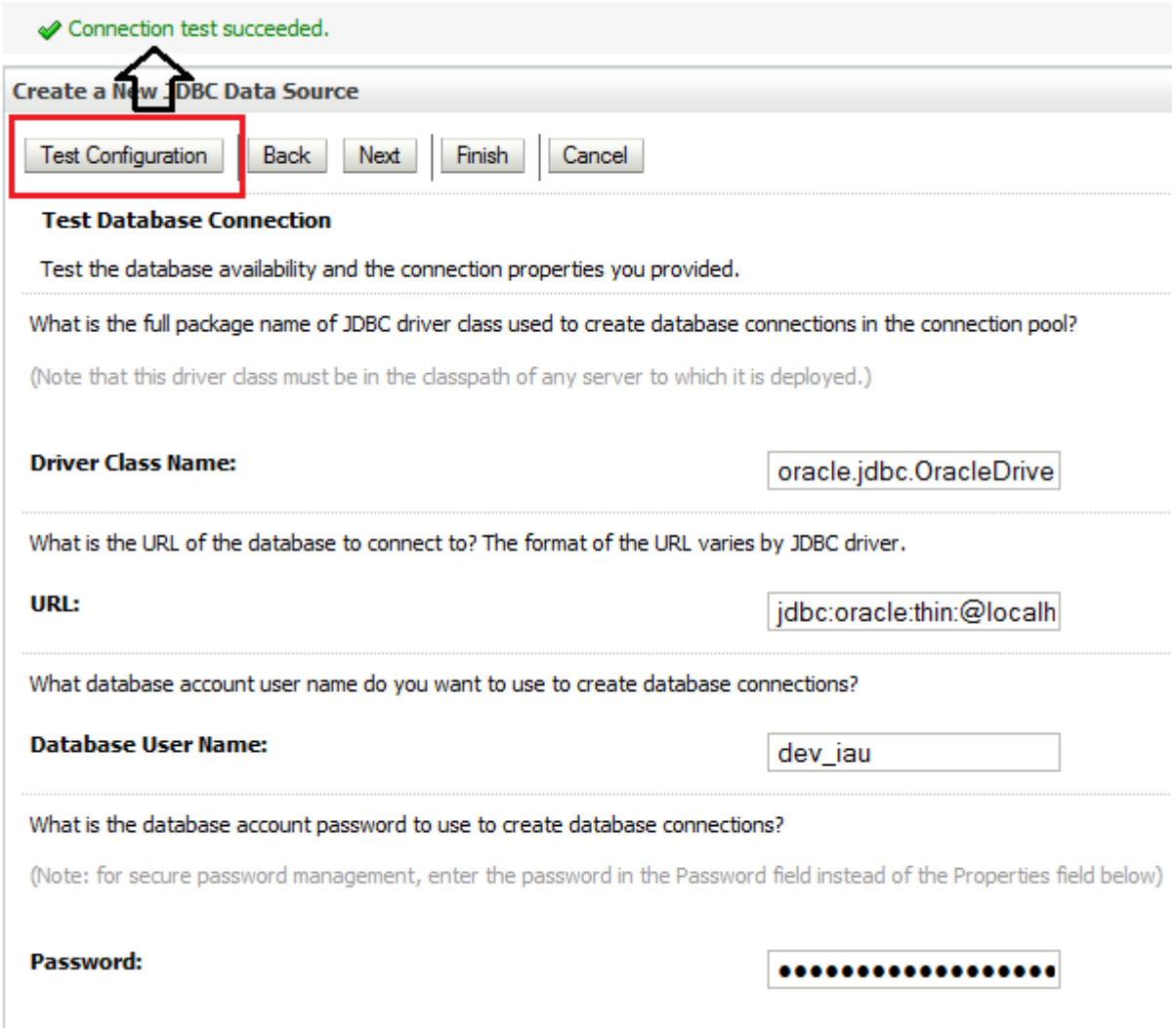


Default Selections

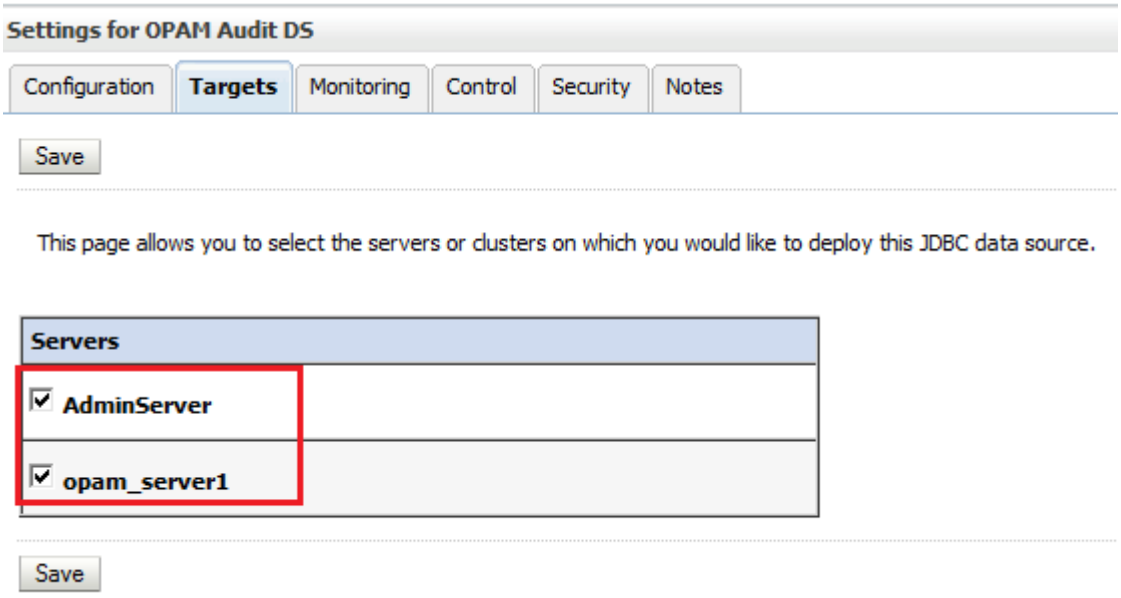


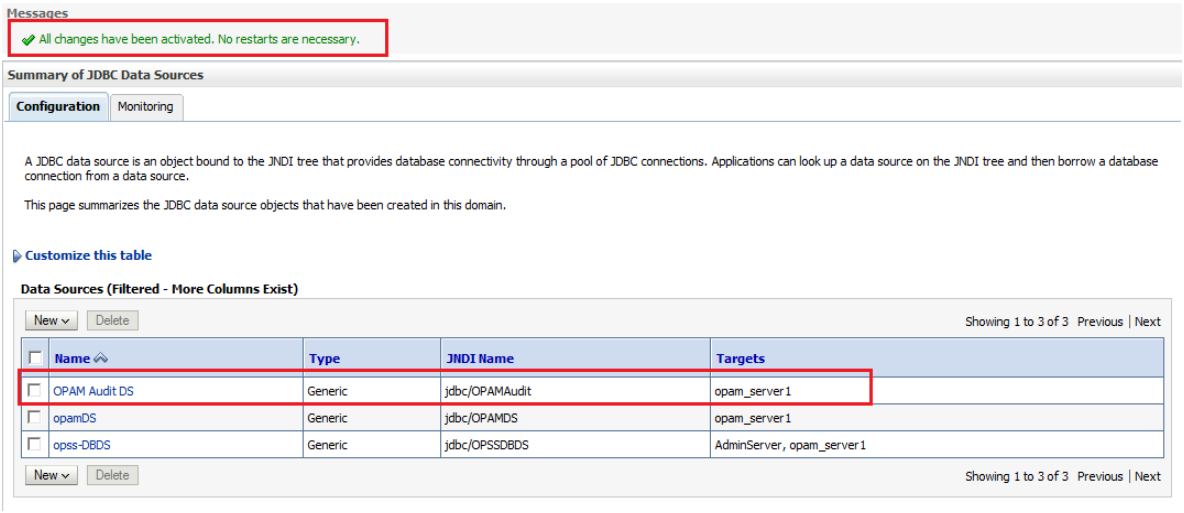


Test the connection



By Abhishek Gupta



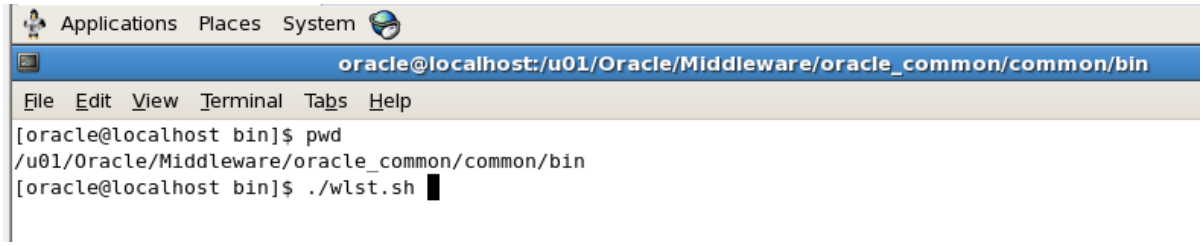


3. **Configure OPAM to use Database centric audit logging**

Initiate WLST

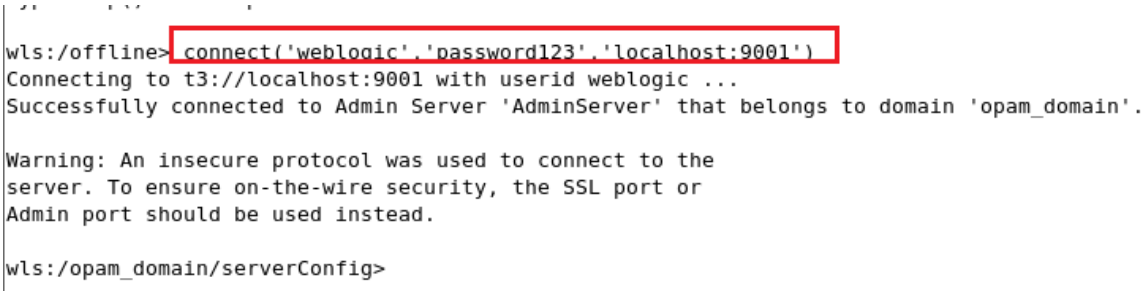
cd /u01/Oracle/Middleware/oracle_common/common/bin

./wlst.sh



On the WLST console, execute below commands

connect('weblogic','password123','localhost:9001')



As of now, we will configure OPAM for MAXIMUM AUDIT logging level

setAuditPolicy(filterPreset='All')

```
wls:/opam_domain/serverConfig> setAuditPolicy(filterPreset='All')
Location changed to domainRuntime tree. This is a read-only tree with DomainMBean as the root.
For more help, use help(domainRuntime)

Audit Policy Information updated successfully
Server need to be restarted for the changes to take effect
wls:/opam_domain/serverConfig>
```

Configure DB as the audit repo

setAuditRepository(switchToDB='true')

```
wls:/opam_domain/serverConfig> setAuditRepository(switchToDB='true')

Audit Repository Information updated
Server need to be restarted for the changes to take effect
wls:/opam_domain/serverConfig>
```

Restart OPAM Admin and Managed servers